

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Richmond Division

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:

SEVEN (7) ACCOUNTS DESCRIBED IN  
ATTACHMENT A

THAT IS STORED AT PREMISES  
CONTROLLED BY APPLE INC.

Case Number 3:21-sw- 57

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent Robert Glore, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with the following accounts:

- creeptor@icloud.com (Target Account 1)
- creeptor.ipad@icloud.com (Target Account 2)
- v\_muradyan@icloud.com (Target Account 3)
- nataliyaohana777@icloud.com (Target Account 4)
- prizegarnitskyj5@gmail.com (Target Account 5)
- eliz-78@mail.ru (Target Account 6) and
- creeptor.tab2@gmail.com (Target Account 7)

(hereafter collectively referred to as “the **TARGET ACCOUNTS**”) that are stored at premises controlled by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California

2. The information to be searched is further described in the following paragraphs and Attachment A. This Affidavit is made in support of an Application for a search warrant

under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. Attachments A and B are attached hereto and incorporated by reference.

3. I am a special agent with the United States Secret Service (USSS) and have been so employed since February 2018. I was previously employed by the USSS as a special agent from March 2003 to August 2014. During my tenure with the USSS, I have participated in numerous search warrants. I have personally conducted and assisted other USSS special agents, as well as other law enforcement officers, in financial and cyber investigations. I have also participated in witness interviews and investigations involving bank fraud, mail fraud, wire fraud, money laundering, and computer crimes.

4. I also worked full-time for over three years as a special agent for the Internal Revenue Service, Criminal Investigation (“IRS-CI”) and was employed in that capacity from August 2014 to February 2018. I was assigned to IRS-CI’s Washington, DC Field Office. My responsibilities included the investigation of the Internal Revenue Code and other related offenses. I personally conducted and assisted other IRS-CI special agents, as well as other law enforcement officers, in tax and non-tax investigations. I also participated in witness interviews and investigations involving bank fraud, mail fraud, wire fraud, money laundering, and computer crimes.

5. During my employment with the USSS, I have received significant training in the investigation of electronic crimes, specifically the forensic analysis of digital evidence including

hardware and software techniques. I received the designation of Electronic Crimes Special Agent (ECSA) and I completed the ECSA training at the Federal Law Enforcement Training Center in Glynco, Georgia, in March 2006.

6. I graduated from the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, in October 2003. I also graduated from the Special Agent Investigative Techniques program at the National Criminal Investigation Training Academy in December 2014. In these programs, I studied a variety of law-enforcement-related classes, criminal investigator, and tax crime issues, including constitutional law, search and seizure, violations of the Internal Revenue laws, and Internal Revenue Service procedures and policies in criminal investigations. During this training, I completed classes in the following subject matter areas: criminal tax issues, money laundering, search and seizure warrants, investigative techniques, methods of proof, and other financial crime related topics.

7. The facts and information contained in this Affidavit are based upon my personal knowledge of the investigation, observations of other law enforcement officers and agents involved in this investigation, and information provided by known sources of information. All observations referenced below that I did not personally make were related to me by the persons who made such observations. Moreover, this Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on the facts as set forth in this Affidavit, I submit that there is probable cause to believe that the information described in Attachment A contains evidence of violations of federal criminal law, including access device fraud (18 U.S.C. § 1029), unauthorized

computer access (18 U.S.C. § 1030), conspiracy, (18 U.S.C. § 371), and conspiracy to commit wire and bank fraud (18 U.S.C. § 1349), as described in Attachment B.

### **JURISDICTION**

9. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **DEFINITIONS**

10. The term “cybercrime forum” refers to websites where people involved in cybercrime come together to discuss and commit criminal activities typically related to payment card fraud, computer hacking, and other related criminal activity. Generally, forum members register anonymously by creating a moniker, and will typically enter an email address during the registration process in order to receive correspondence related to forum activity, or as a means of account recovery if they forget their password or are locked out of their accounts.

11. An “Internet Protocol address” or “IP address” is a numerical address assigned to each computer connected to a network that uses the internet for communication. Because every device that connects to the internet must use an IP address, IP address information can help to identify which computer or other device was used to access an account. Email providers, internet providers, and even cybercrime forums often record the IP address used to register an account and the IP addresses associated with particular logins to the account.

12. “Jabber” is a protocol for creating real-time, text-based communications that allows users to create their own chat service hosted on computers of their own choosing. Jabber account addresses look similar to email addresses with an account identifier preceding the “@”



symbol, followed by a domain address associated with the Jabber server. Because Jabber accounts can be created and hosted by cybercriminals themselves, it is often a favored method of communication for cybercriminals.

13. “Cryptocurrency,” also referred to as “digital currency” or “virtual currency,” is a financial asset that exists only in digital form. Cryptocurrencies share some of the characteristics of traditional money, i.e., “fiat currency,” which is typically backed by a central government, but do not have a physical equivalent in the real world. The types of digital currencies available are constantly growing and changing, but examples of major cryptocurrencies in use today include Bitcoin, Ethereum, Ripple, Litecoin, Tether and Monero, among others. The name “cryptocurrency” comes from the strong cryptography that is used to secure records of transactions for a particular digital currency. Some of these currencies are centralized, where a group of people and computers regulate the transactions, and others are decentralized, where there is no controlling group or computers. Many forms of digital currencies can be exchanged for the fiat currency of one country or another through an exchange service.

14. The term “card checking service” refers to a criminal service that checks credit or debit cards stolen by other criminals to see if they are still valid and can be used to make purchases. Operators of card checking services have a back door way of checking the cards through payment card networks. Card checking services often have a website that allows customers to check their cards in exchange for payment. Card checking services also rent their checking ability directly to stolen credit card vending websites so the credit card vendors can integrate the checking with their shop.

15. The term “moniker” refers to the chosen online name of a cybercriminal. Based on my training and experience, I know that cybercriminals often use the same online moniker or

nickname to identify themselves online. Because cybercriminals often communicate over the internet without divulging their true identity, many use one or more monikers frequently to generate a “brand” or consistent identity in their online interactions. Using the same moniker across platforms allows such criminals to enter into illegal transactions more effectively, like selling code, anonymously online by generating goodwill and credibility around their use of their moniker. Frequently, a cybercriminal’s moniker will be incorporated into account names for online communication services, such as instant messaging platforms or email addresses, or for accounts on online criminal forums.

### **PROBABLE CAUSE**

16. The USSS is investigating an unknown individual who goes by the online moniker “Creeptor.” Based chiefly on electronic evidence obtained from a convicted cybercriminal’s device, and communications between cybercriminals, investigators believe Creeptor along with other co-conspirators run several automated web-stores that sell personally identifiable information (PII), such as names, addresses, dates of birth and social security numbers, as well as access device data. Specifically, Creeptor appears to be the coder that designs and maintains the websites and pays for the hosting and services the websites use.

17. As detailed below, the **TARGET ACCOUNTS** have been identified as being associated with Creeptor and are likely to contain information that will support the further identification of Creeptor and other possible co-conspirator(s), and provide further information about criminal activities.

#### ***A. Initial Identification of the Creeptor Moniker and Use of that Moniker in Connection with Cyber Crime***

18. In July 2019, a Ukrainian cybercriminal (cooperating defendant) identified as C.D. pled guilty in the United States District Court for the Eastern District of Virginia to crimes

related to the trafficking of stolen PII and stolen payment card data, participating in reshipping schemes, and operating a card-checking service. Prior to, and after, their guilty plea, C.D. provided information to the United States regarding their ten-year involvement in cybercrime. For example, C.D. voluntarily provided a laptop computer containing their communications with other cybercriminals and other records of their activities dating from approximately 2009 through 2019.

19. A forensic examination of C.D.'s computer revealed the monikers, or online nicknames, of individuals C.D. had communicated with in connection to cybercrime. Those monikers included Creeptor, which C.D. identified as the moniker operated by a person who was a co-conspirator who helped run a joint criminal business that sold stolen PII and payment card data through automated webstores.

20. As part of C.D.'s cooperation with the United States, federal agents periodically provide C.D. with a computer and internet access for limited durations of time during which agents closely supervise C.D.'s cooperation. Outside of these periods of supervision, C.D. does not have access to a computer or the internet. During these sessions, federal agents have supervised C.D.'s Jabber communications with several former co-conspirators. On or about June 13, 2019, Creeptor and C.D. had a Jabber conversation. Creeptor stated that he received a new set of cards. Creeptor shared the cards via a link to the online file sharing service Sendspace. The file contained approximately 8,000 payment card numbers with corresponding information about the cardholders.

21. The card numbers were submitted to the National Cyber Forensics and Training Alliance and its bank partners. Approximately 5,004 cards were from potential US victims with an initial loss amount on those cards of approximately \$2,502,000. J.P. Morgan Chase bank



provided actual losses of \$22,088 on 88 cards and American Express provided actual losses of \$27,838 on 185 cards issued to US persons.

***B. Evidence Showing Creeptor Monikers Are Connected to Cybercrime and Associated with the TARGET ACCOUNTS***

22. The USSS further reviewed records from cybercrime forums (described herein as Forum 1 and Forum 2) related to the Creeptor moniker, these records included the email address used to register for the Creeptor accounts – creeptor@gmail.com

23. Forum 1 and Forum 2 are online forums whose membership is limited to Russian-speaking cybercriminals who can demonstrate their criminal bona fides (typically in the form of references from other established cybercriminals who are already forum members). Law enforcement obtained Forum 1 records pursuant to a Mutual Legal Assistance Treaty with the Netherlands in 2014. Forum 1 records contained data associated with accounts registered under the Creeptor moniker. The Creeptor account was registered with the creeptor@gmail.com email address. Forum 2 records were obtained pursuant to a Mutual Legal Assistance Treaty with Netherlands in 2015. Forum 2 records included data associated with accounts registered under Creeptor moniker, and that account was also registered using the creeptor@gmail.com email address.

24. I reviewed public posts and private messages associated with Creeptor moniker on Forum 1 and Forum 2, and my review of the communications indicated that the owner of the two accounts discussed computer coding and hacking. Another post appears to provide 12 Visa access devices with the corresponding names, addresses, and emails. Because email addresses associated with cybercrime forums often contain notifications from the forums, there is reason to believe that the email addresses discussed in this section may contain evidence of crimes



associated the Creeptor accounts, and in particular, crimes associated with the laundering of criminal proceeds.

25. I reviewed IP address connection data received from legal process to Google and Apple for email addresses creeptor@gmail.com and creeptor@icloud.com (**Target Account 1**), creeptor.ipad@icloud.com (**Target Account 2**) and creeptor.tab2@gmail.com (**Target Account 7**). The IP's of 46.133.28.243, 128.124.152.186, 188.191.237.49, 188.191.237.5, 185.189.185.198, and 188.191.238.154 were identified as accessing multiple different email addresses along with the creeptor@gmail.com and/or one or more of the **TARGET ACCOUNTS** on the same date.

26. The IP address that created the creeptor@gmail.com email account on September 24, 2008, was 195.182.193.194. This same IP address also created the following nine other Google email address accounts from September 23, 2008, to October 1, 2008:

<b>Email Accounts:</b>
<b><u>alya.v.alex@gmail.com</u></b>
<b><u>idaymon88@gmail.com</u></b>
<b><u>zodchi8888@gmail.com</u></b>
<b><u>vasiliv.ukr@gmail.com</u></b>
<b><u>spomorcev@gmail.com</u></b>
<b><u>Alenka2102@gmail.com</u></b>
<b><u>valik.pylypko@gmail.com</u></b>
<b><u>abensesearl@gmail.com</u></b>
<b><u>loshooliguns@gmail.com</u></b>

27. Through my training and experience, I know that cybercriminals typically use multiple email addresses to execute their schemes. Most legitimate and criminal internet services require an email address to register. Because email addresses are free to create, cybercriminals tend to create several email addresses and use them to register different services.

This practice makes it more difficult for investigators to track different activities to the same email address and effectively track different criminal activities to the same account holder.

28. Through my review of law enforcement indices and publicly available sources, I determined that IP address 195.182.193.194 is owned by an internet service provider located in Chernivtsi, Ukraine, which is the city where I believe the person using the Creeptor moniker lives. Currently it is unknown whether that IP address is assigned to a residence or commercial location. While it is possible that the 195.182.193.194 IP address is publicly available, it appears more likely than not that at least some of the above-listed email addresses created using that IP address were created by the person using the Creeptor moniker. I base this conclusion on the relatively short time span over (8 days) which all of these email addresses, including creeptor@gmail.com, were created using the same IP address, as well as the discussion herein regarding cybercriminals creating and using multiple email accounts.

29. In addition, cybercriminals also often maintain separate accounts for their legitimate and criminal activities. However, most legitimate email services require recovery email addresses or cell phone numbers to enable users to access the account if a password is forgotten or misplaced, or to enable two-factor authentication. Like law-abiding users of online accounts, cybercriminals will very often designate one of their main personal email accounts as a recovery account so that they can quickly notice unusual activity on the account and more easily reset or regain access to their criminal email account in the event of a problem. Investigators can often connect a criminal's multiple emails accounts to one another because they may be linked by a common IP address, cell phone number or recovery email address that was used to register them. In addition, based on my experience and training, I know that cybercriminals often transfer information between a primary email account and their linked, or recovery, email

accounts. The TARGET ACCOUNTS will probably contain evidence or identifying information related to criminal activity.

**C. *Information about Activity Linked to TARGET ACCOUNTS and Use of Email Accounts by Cybercriminals in Connection to Cybercrime Forum Activity and Cybercrime***

30. On or about February 18, 2020, Google provided records pursuant to legal process for the creepor@gmail.com email address. The creepor@gmail.com email address was registered in the name of Александр Максимович (translated as Aleksandr Maksimovich). The account was created on or about September 24, 2008, and was active at the time of the response from Google. The account was last accessed on or about February 3, 2020. The account is linked to a Ukrainian Phone +380997504171.

31. Business records obtained from Google pertaining to an account named creepor.tab2@gmail.com indicate it was registered in the name of Александр Максимович (translated as Alexander Maksimovich). The account was created on or about March 28, 2013, and was active at the time of the response from Google. The recovery email address for the account was creepor@gmail.com.

32. Business records obtained from Apple pertaining to the creepor@gmail.com email address indicate a subscriber name of Александр Максимович (translated as Alexander Maksimovich), with a street address of Ольжи 10 (translated as Olzhi 10) city of Черновцы (translated as Chernivtsi) Ukraine 58003, business phone number: 1 099 7504171, DSID (Directory Services Identifier)<sup>1</sup> 10884939974, and associated email address of

---

<sup>1</sup> DSID or Directory Services Identifier is a method of identifying AppleID accounts. It is an equivalent to a serial number for a device, however it is assigned to an AppleID or iCloud account for use in identifying cases in iLog, the iCloud support tool, or for verifying a customer over the line.



creeptor@icloud.com (**Target Account 1**). Records from Apple list this account holder as the registered owner of the following devices: 1) Apple MacBook, serial number C02ST025GTHT; 2) Apple MacBook Pro, serial number C02VC1HKHTD6; and a 3) Apple iPhone-11, serial number F17ZG20FN6Y9. Alexander Maksimovich is also the registered owner of an Apple iPad, serial number F9HZGD13MF3M, DSID: 17115338848, using the email address of creeptor.ipad@icloud.com (**Target Account 2**). The creeptor@icloud.com (**Target Account 1**) account was created on February 24, 2017, and was active on April 10, 2020. The creeptor.ipad@icloud.com (**Target Account 2**) account was created on January 25, 2020, and was active on April 13, 2020.

33. When a user registers on a cybercrime forum, the user usually receives a confirmation message via the email they input during the registration process. Cybercriminals often also receive other notifications from the cybercrime forums through email and share these confirmation requests with multiple emails and/or electronic devices. Thus, because the creeptor@gmail.com email address was used in the registration of monikers on known cybercrime forums, it is likely that the account confirmation and other notifications from the cybercrime forums were sent to one or more of the **TARGET ACCOUNTS**.

34. Further, cybercriminals typically set up email notifications for themselves to receive alerts when co-conspirators send them messages using platforms such as Jabber. In this investigation, Creeptor has used multiple Jabber addresses to communicate with cooperators during federal undercover communications via Jabber. Thus, it is likely that one or more of the **TARGET ACCOUNTS** may contain evidence of communications with co-conspirators regarding the exchange of illegal services; evidence of their crimes; or evidence of the scope of their crimes.



35. A review of records received from Apple relating to activity connected to the IP address of 46.133.28.243 on April 25, 2019, with time stamps of 01:55:34 and 02:02:22 Pacific Time identified a user with a person id: 8180689425, device type name: “iPhone 6,1,” device id and/or global unique id (GUID)<sup>2</sup> of 5d3737b8c0bbc15b3d7618969864c6956de4972f. Apple records listed the registered user for this device as Vova Muradyan with a street address of St Oljicha 30, Kit omit, Ukraine 10800, email address: [prizegarnitskyj5@gmail.com](mailto:prizegarnitskyj5@gmail.com) (**Target Account 5**), phone number: 097 0072015. The [prizegarnitskyj5@gmail.com](mailto:prizegarnitskyj5@gmail.com) (**Target Account 5**) account was created on January 2, 2015, and was active as recently as February 1, 2020.

36. The IP address of 46.133.28.243 is registered to PrJSC "VF UKRAINE" 15, Leiptsigaska str., Kyiv, Ukraine, 01601, +380442300257. The company is a subsidiary of MTS, a large Russian telecommunications company, which is operated by Vodafone. This suggests to me that the IP address 46.133.28.243, which figures prominently in this affidavit, is not associated with an Internet café or unsecured residential Wi-Fi router. I would note that the registered user for this device and the email address [prizegarnitskyj5@gmail.com](mailto:prizegarnitskyj5@gmail.com) (**Target Account 5**), i.e., “Vova Muradyan,” has a first initial and last name identical to [v\\_muradyan@icloud.com](mailto:v_muradyan@icloud.com) (**Target Account 3**).

---

<sup>2</sup> GUID is short for “Globally Unique Identifier.” A GUID is a 128-bit (16-byte) number generated by software programs to uniquely identify a particular component, data object, application, file, database entry and/or a user. There is no central registry of GUIDs, and thus there is no guarantee that any particular GUID is truly unique in the universe. However, if generated using standard methods, the likelihood of the same GUID being duplicated for two different things is close enough to zero to be negligible.

37. Further review of Apple records identified a subscriber name of Вова Мурадян (translated as Vova Muradyan) with a street address of Ольжича (translated as Olzhicha) city of Житомир (translated as Zhytomyr) Ukraine 10010, business phone number 1 097 8685839, DSID 11603570631, email address v\_muradyan@icloud.com (**Target Account 3**), as the registered owner of the following device: Apple iPhone 7, serial number F71V46KMHG7F. The v\_muradyan@icloud.com (**Target Account 3**) account was created on October 19, 2017, and was active as recently as April 23, 2020.

38. A review of Apple records for the IP address of 178.133.44.179 on March 7, 2019, with time stamp 07:33:05 GMT identified the account of prizegarnitskyj5@gmail.com (**Target Account 5**) in the name of Vova Muradyan accessing Apple services. This same IP address (178.133.44.179) was also accessing the account of eliz-78@mail.ru (**Target Account 6**) in the name of Vova Muradyan on the same day, March 7, 2019, less than one minute earlier at 07:32:23 GMT for Apple services. The eliz-78@mail.ru (**Target Account 6**) account was created on January 2, 2015, and was active as recently as March 7, 2019. The IP address of 178.133.44.179 is registered to PrJSC "VF UKRAINE," the subsidiary of a large Russian telecommunications company. Like the discussion in paragraph 36 above regarding IP address 46.133.28.243, this indicates to me that the IP address 178.133.44.179 is not associated with an Internet café or unsecured residential Wi-Fi router.

39. Additional review of Apple records for the GUID of 5d3737b8c0bbc15b3d7618969864c6956de4972f (see paragraph 35 above) identified an Apple iPhone 5S space gray 16GB with serial number DX4NMLFFFNJJ. This Apple iPhone 5S was registered on or about January 2, 2015, to Dima Dmitruk, mail address 1: Monstersk, city: Lol, Ukraine, 17399, business phone number 1 099 5328836, email address

prizegarnitskyj5@gmail.com (**Target Account 5**). This same iPhone was also registered on or about August 2, 2019, to Наташа Охана (translated as Nataša Ohana), mail address 1 Хлебная (translated as bread), City:Житомир (translated as Zhytomyr), Ukraine, 20010, business phone number 1 098 0857775, email address nataliyaohana777@icloud.com (**Target Account 4**). The nataliyaohana777@icloud.com (**Target Account 4**) account was created on August 2, 2019, and was active on April 23, 2020. This same GUID: 5d3737b8c0bbc15b3d7618969864c6956de4972f and person id: 8180689425 activated Apple accounts for subscribers' eliz-78@mail.ru (**Target Account 6**) and prizegarnitskyj5@gmail.com (**Target Account 5**) on or about January 2, 2015, in the names of Vova Muradyan and Dima Dmitruk. On or about August 2, 2019, the same GUID: 5d3737b8c0bbc15b3d7618969864c6956de4972f activated an Apple account for person id: 16767124957 and email address nataliyaohana777@icloud.com (**Target Account 4**) for Apple subscriber Наташа Охана (translated as Nataša Ohana).

40. The GUID of 5d3737b8c0bbc15b3d7618969864c6956de4972f activated multiple Apple accounts using: 1) person id 8180689425, email address prizegarnitskyj5@gmail.com (**Target Account 5**) for Apple subscriber Vova Muradyan; 2) person id 16767124957, email address nataliyaohana777@icloud.com (**Target Account 4**) for Apple subscriber Наташа Охана (translated as Nataša Ohana); and 3) person id 8180689425, email address eliz-78@mail.ru (**Target Account 6**) for Apple subscriber Vova Muradyan. The same person id 8180689425 registered different Apple subscriber accounts on January 2, 2015: 1) Vova Muradyan with email addresses: prizegarnitskyj5@gmail.com (**Target Account 5**) and eliz-78@mail.ru (**Target Account 6**) and 2) Dima Dmitruk with email address: prizegarnitskyj5@gmail.com (**Target Account 5**). The Apple subscriber accounts of Vova Muradyan and Dima Dmitruk are using the same e-mail address of prizegarnitskyj5@gmail.com (**Target Account 5**). The Apple subscriber



Vova Muradyan is also the account holder for three different email addresses:

prizegarnitskyj5@gmail.com (**Target Account 5**), eliz-78@mail.ru (**Target Account 6**), and v\_muradyan@icloud.com (**Target Account 3**).

41. Review of records from Google and Apple revealed the creepor@gmail.com account and the prizegarnitskyj5@gmail.com (**Target Account 5**) account accessed the Internet from the same IP address (46.133.28.243) on April 25, 2019. On that date, Google logged 122 events<sup>3</sup> for the creepor@gmail.com account, and Apple logged 14 events for the prizegarnitskyj5@gmail.com (**Target Account 5**) account.

42. Records received from Apple and Google show that another shared IP address was used later to access the creepor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**) accounts within one day of each other. Those records show that the creepor@gmail.com account was accessed from IP address 46.133.232.237 on May 6, 2019, at 13:15:38 UTC (Coordinated Universal Time, also known as Greenwich Mean Time), which was approximately 4:15 p.m. local time in Ukraine. On May 7, 2019, almost exactly 24 hours later, the prizegarnitskyj5@gmail.com (**Target Account 5**) account was accessed from IP address 46.133.232.237 at 13:16:54 UTC, or 4:16 p.m. local time in Ukraine. Records show that IP address 46.133.232.237 is also registered to PrJSC “VF UKRAINE,” the subsidiary of a large Russian telecommunications company. Again, the fact that this IP address is owned by a

---

<sup>3</sup> In computer programming, an event is an action that occurs as a result of input from the user or another source, such as a mouse click on a button within a web page, a web browser completely loading a web page, or a hardware sensor such as a microphone or speaker receiving sensory input, to name just a few.



large telecommunications provider indicates to me that these accounts were not accessed from an unsecured residential Wi-Fi router or an Internet café.

43. Additional records obtained from Apple further link the prizegarnitskyj5@gmail.com (**Target Account 5**) account to the eliz-78@mail.ru (**Target Account 6**) and nataliyaohana777@icloud.com (**Target Account 4**) accounts by shared IP addresses. On March 7, 2019, Apple logged 41 events for the prizegarnitskyj5@gmail.com (**Target Account 5**) account and 6 events for the eliz-78@mail.ru (**Target Account 6**) account all from the same IP address of 178.133.44.179. On January 6, 2020, Apple logged 14 events for the prizegarnitskyj5@gmail.com (**Target Account 5**) account and 7 events for the nataliyaohana777@icloud.com (**Target Account 4**) account all from the same IP address of 46.211.233.176.

44. A review of Apple sign-on records for the IP address of 128.124.152.186 for January 20, 2020, with time stamps from 10:07:08 to 10:08:04 GMT identified a user with Apple person id: 10884939974. As discussed in paragraph 32 above, the person id 10884939974 is associated with the Ukrainian customer name Александр Максимович (translated as Alexander Maksimovich). Maksimovich is the subscriber for creeptor@icloud.com (**Target Account 1**). This same IP address (128.124.152.186) was also accessing the creeptor@gmail.com account on January 20, 2020. The IP address of 128.124.152.186 is registered to PrJSC "VF UKRAINE," the subsidiary of a large Russian telecommunications company.

45. A review of Apple records for the IP address of 188.191.237.49 on October 12, 2019, with time stamp 12:50:43 GMT identified sign-on records for account name and Apple credential id creeptor@icloud.com (**Target Account 1**) and the DSID/person id 10884939974. As previously noted, Apple records indicate that this DSID/person id is connected to Alexander

Maksimovich, the subscriber of creeptor@icloud.com (**Target Account 1**). This same IP address (188.191.237.49) was also used to access creeptor@gmail.com account on October 12, 2019. The IP address of 188.191.237.49 is registered to Intelekt, a Ukrainian Internet service provider.

46. A review of Apple records for the IP address of 188.191.237.5 on October 13, 2019, with time stamp 03:15:44 PST/PDT identified a connection by a device with DSID/person id: 10884939974, GUID 00008030-001024303E08802E, and associated email address creeptor@icloud.com (**Target Account 1**). Again, this DSID is registered to Alexander Maksimovich, the listed subscriber for creeptor@icloud.com (**Target Account 1**). This same IP address (188.191.237.5) also accessed the creeptor@gmail.com account on October 13, 2019, and is also registered to the Ukrainian service provider Intelekt.

47. A review of Apple records for the IP address of 185.189.185.198 on January 28, 2020, with time stamp 15:05:55 PST/PDT identified a connection by a device with the DSID/person id: 17115338848, and associated email address creeptor.ipad@icloud.com (**Target Account 2**). As reflected in paragraph 32 above, this DSID is registered Alexander Maksimovich of Ukraine. This same IP address (185.189.185.198) also accessed the creeptor@icloud.com (**Target Account 1**) account on January 28, 2020. The IP address of 185.189.185.198 is registered to the Ukrainian service provider Intelekt.

48. A review of Apple records for the IP address of 188.191.238.154 on January 25, 2020, with time stamp 3:16:43 PST/PDT showed a connection by an account/device with the DSID/person id: 17115338848 and email address creeptor.ipad@icloud.com (**Target Account 2**), which is registered to Alexander Maksimovich. This same IP address (188.191.238.154) also accessed the creeptor.tab2@gmail.com (**Target Account 7**) account on January 25, 2020. The

IP address of 188.191.238.154 is registered to the Ukrainian service provider Intelekt. Also on January 25, 2020, at time 17:10:40 PST/PDT, the same IP address (188.191.238.154) was used by device with GUID 00008030-001024303E08802E, associated email address:

creepor@icloud.com (**Target Account 1**), and DSID/person id 10884939974. As indicated in paragraph 46 above, this GUID is associated with Alexander Maksimovich, the registrant of email address creepor@icloud.com (**Target Account 1**). As reflected in paragraph 32 above, information from Apple connects DSID 10884939974 to Alexander Maksimovich.

49. A review of emails contained in the creepor@gmail.com account received from Google on or about February 18, 2020, identified Apple products that were signed and/or registered using this email account. Google also provided account sign on records including IP addresses for the creepor@gmail.com account. An additional email dated January 25, 2020, also identified a new sign-in to a linked account of creepor.tab2@gmail.com (**Target Account 7**) using a new Apple iPad device. A comparison of the Apple product sign-in and/or registration emails with the Google account sign-in IP addresses revealed:

Email	Date / Time	Action / Message from Apple	IP address
<u>creepor@gmail.com</u>	2/27/2019 17:40 UTC	Signed in to account on new device  <u>creepor@gmail.com</u>  Your Google Account has just been signed in on your <b>new Mac device</b> . We want to make sure that it was you.	37.252.5.86
<u>creepor@gmail.com</u>	6/19/2019 12:39 UTC	Signed in to account on new device  <u>creepor@gmail.com</u>  Your Google Account has just been signed in on your <b>new Mac device</b> .	51.75.56.78 and/or 91.199.245.254



Email	Date / Time	Action / Message from Apple	IP address
		We want to make sure that it was you.	
<a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a>	10/12/2019 14:12 UTC	Sign in to your account on a new device  <a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a>  Your Google Account has just been signed in on your <b>new Apple iPhone</b> . We want to make sure that it was you.	188.191.237.49
<a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a>	10/12/2019 14:13 UTC	Hello, Alexander! You are signed in with your <b>new Apple iPhone</b> Complete the setup of your <b>Apple iPhone</b> and install these official Google apps.	188.191.237.49
<a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a>	10/13/2019 10:16 UTC	Sign in to your account on a new device  <a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a>  Your Google Account has just been signed in on your <b>new Apple iPhone</b> . We want to make sure that it was you.	188.191.237.5
<a href="mailto:creeptor@gmail.com">creeptor@gmail.com</a> and/or <a href="mailto:creeptor.tab2@gmail.com">creeptor.tab2@gmail.com</a>	1/25/2020 10:21 UTC	New sign-in to your linked account  <a href="mailto:creeptor.tab2@gmail.com">creeptor.tab2@gmail.com</a> Your Google Account was just signed in to from a <b>new Apple iPad device</b> . You're getting this email to make sure it was you.	46.133.124.238 and/or 188.191.238.154

50. A review of emails contained in the [creeptor@gmail.com](mailto:creeptor@gmail.com) account identified at least two emails indicating the use of Apple Pay, which is a mobile payment and digital wallet

service by Apple and which further suggests the likely use of an Apple iCloud account. Those emails were as follows:

- a. Dated October 13, 2019, stating "Alexander Maksimovich, congratulations! Your card \*\*\*\*4\*83 is activated in Apple Pay!"
- b. Dated November 28, 2019, stating "Alexander Maximovich! Your \*\*\*\*8283 card was reissued and we automatically upgraded it to the new \*\*\*\*9333 on Apple Pay."

51. A review of Apple records identified an Apple Pay subscriber account in the name Александр Максимович (translated as Alexander Maksimovich), with a street address of Ольжи 10 (translated as Olzhi 10) city of Черновцы (translated as Chernivtsi) Ukraine 58003, phone number: +3800997504171, Apple id: [creeptor@icloud.com](mailto:creeptor@icloud.com) (**Target Account 1**). The issuing bank for the Apple Pay account was the OJSC Universal Bank. The Apple Pay account was activated on or about November 29, 2019, on an iPhone 11 Pro, serial number: F17ZG20FN6Y9, registered to Александр Максимович (translated as Alexander Maksimovich).

**SUMMARY OF EVIDENCE CONNECTING THE USER OF  
CREEPTOR-NAMED ACCOUNTS TO OTHER TARGET ACCOUNTS**

52. Based on the information above, I believe the same individual controls all seven TARGET ACCOUNTS. As discussed earlier, it is common tradecraft among cybercriminals to create and use multiple email accounts as part of their criminal schemes. The most frequent purpose for this is concealment of the perpetrator's identity. While using the same name or moniker in multiple forums can serve a branding purpose that a cybercriminal may find advantageous at times, there are other instances where cybercriminals may seek to

compartmentalize their activities vis-à-vis certain individuals or organizations in order to prevent easy linkage, which is where multiple email accounts can be beneficial.

53. The evidence above strongly suggests that all of the accounts with Creeptor-derived names, i.e., creeptor@gmail.com, creeptor.tab2@gmail.com (**Target Account 7**), creeptor@icloud.com (**Target Account 1**) and creeptor.ipad@icloud.com (**Target Account 2**), were created and are used by the same individual. Business records indicate that the subscriber for all these accounts is Alexander Maksimovich, who lists a residence in Ukraine. On multiple occasions two or more of these accounts were accessed through the same IP address on the same date. The recovery email account for these accounts is creeptor@gmail.com. Given the creeptor@gmail.com account's link to multiple online forums dedicated to criminal carding, the evidence strongly suggests that Alexander Maksimovich is the cybercriminal with the moniker Creeptor who controls all of these accounts.

54. The evidence further indicates that the other TARGET ACCOUNTS, specifically prizegarnitskyj5@gmail.com (**Target Account 5**), eliz-78@mail.ru (**Target Account 6**), nataliyaohana777@icloud.com (**Target Account 4**), and v\_muradyan@icloud.com (**Target Account 3**) were created and are used by the same individual. The same GUID of 5d3737b8c0bbc15b3d7618969864c6956de4972f is linked to the activation of the prizegarnitskyj5@gmail.com (**Target Account 5**), eliz-78@mail.ru (**Target Account 6**) and nataliyaohana777@icloud.com (**Target Account 4**) accounts. (See paragraphs 35, 39 and 40 above.) As discussed in Footnote 1, a GUID is a computer-generated unique identifier used to identify a particular user or a piece of information in a computer system. The probability that different individuals randomly obtained the same computer-generated GUID and activated the prizegarnitskyj5@gmail.com (**Target Account 5**), eliz-78@mail.ru (**Target Account 6**) and



nataliyaohana777@icloud.com (**Target Account 4**) accounts is statistically close to zero. (See footnote 2.) Shared IP address activity, all through IP address 178.133.44.179, further links these three accounts together. (See paragraphs 38 and 43 above.)

55. Subscriber records from Apple show that the same person, Vova Muradyan, is the account holder for the prizegarnitskyj5@gmail.com (**Target Account 5**), eliz-78@mail.ru (**Target Account 6**), and v\_muradyan@icloud.com (**Target Account 3**) accounts. (See paragraph 40 above.) Thus, v\_muradyan@icloud.com (**Target Account 3**) is linked to prizegarnitskyj5@gmail.com (**Target Account 5**) and eliz-78@mail.ru (**Target Account 6**) by subscriber name the way nataliyaohana777@icloud.com (**Target Account 4**) is linked to these same accounts by GUID.

56. Finally, the evidence suggests that the creator and user of all the Creeptor-named accounts is also the creator and user of the other TARGET ACCOUNTS. As discussed above, the creeptor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**) accounts all accessed the Internet from the same IP address on April 25, 2019. (See paragraph 41 above.) About one month later, during the period of May 6-7, 2019, the creeptor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**) accounts accessed the Internet just 24 hours apart from the same IP address. (See paragraph 42 above.)

57. Important to my assessment of the relevance of the shared IP addresses is the fact that these IP addresses were registered to cellular network providers. The format for these IP addresses, e.g., 46.133.232.237, is Internet Protocol version 4, or IPv4. For a variety of reasons, including the mathematical limit to the total number of such addresses, rules about their use, and the vast proliferation of devices connecting to the Internet, for years there have not been enough IPv4 addresses to give every device a unique IP address. This shortage of IPv4 addresses

compared to total devices is called “address space exhaustion.” To resolve the problem of address space exhaustion, cellular providers employ an engineering approach known as “carrier-grade NAT” where NAT stands for “network address translation.” A cellular carrier (like AT&T or Verizon) will assign the same IP address to numerous cell phones—indeed, sometimes literally hundreds of devices—all connecting to the Internet at the same time. I do not have direct knowledge of how many devices the telecommunications company PrJSC “VF UKRAINE” would assign to a single IP address. I do know, however, that smart phones are abundant in Ukraine, and the phenomenon of “address space exhaustion” is not unique to the United States. It is reasonable to conclude that at any given moment in Ukraine, tens of thousands of smart phones are connecting to the Internet through hundreds of IP addresses. Given the large number of mobile devices that would have been connecting to the Internet through the same IP address at any given time, it appears to be at least a fair probability that the user(s) of creeptor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**), which both connected to the Internet through the same IP address in close time to each other on at least two different dates, are the same individual.

58. Reinforcing the inferences about the relevance of shared IP addresses pointing toward a single person being the user of creeptor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**) is the existence of multiple related accounts associated with both creeptor@gmail.com and prizegarnitskyj5@gmail.com (**Target Account 5**). The two main groups of TARGET ACCOUNTS (i.e. the Creeptor-named accounts and the other non-Creeptor-named accounts) are connected to an individual who created and uses multiple email accounts, sometimes creating multiple accounts in a short time span (see paragraph 26 above). As discussed above, I know this to be a standard technique of cybercriminals. Additionally, the eliz-

78@mail.ru (**Target Account 6**) and prizegarnitskyj5@gmail.com (**Target Account 5**) accounts were both registered in the same two separate names, i.e., Vova Muradyan and Dima Dmitruk.

59. In addition, based on my experience and training, I know that cybercriminal's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can overlap and help to identify which computers or other devices were used to access the TARGET ACCOUNTS (i.e. the Creeptor-named accounts and the other non-Creeptor-named accounts). Such information also allows law enforcement to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. Law enforcement can often connect a criminal's multiple emails accounts to one another because they may be linked by a common IP Address. In addition, based on my experience and training, I know that cybercriminals often transfer information between a primary email account and their linked, or recovery, email accounts.

### **BACKGROUND ON APPLE**

60. Based on my training and experience, information related to the Apple services used by an Apple user who is a cybercriminal may yield information about their identity, as well



as the scope and nature of their crimes. Through my experience, I also know that cybercriminals typically communicate via email and often store communications with co-conspirators and information about their criminal endeavors within the content of email. In addition, I know, based on my training and experience, that if an Apple Account holder does not delete content, then it will remain in the account, and that cybercriminals often do not delete content in accounts they use, even if those accounts are ones used for only a brief window of time. As a result, the **TARGET ACCOUNTS** likely contain information that will support the further identification of Creeptor and his co-conspirator(s), and provide further information about criminal activities. Therefore, there is probable cause to believe that the **TARGET ACCOUNTS** contain evidence, instrumentalities, and fruits of crimes.

61. In my training and experience, and based on my review of Apple's website, terms of service, and privacy policy, I have learned the following information about Apple.

62. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

63. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

64. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

65. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages")

containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

66. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

67. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

68. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

69. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

70. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System (GPS) networks, and Bluetooth, to determine a user's approximate location.

71. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

72. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

73. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

74. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including



the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the IP address used to register and access the account, and other log files that reflect usage of the account.

75. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

76. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number (ICCID), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (MAC

address), the unique device identifier (UDID), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

77. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

78. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when,

where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

79. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

80. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

81. Account activity may also provide relevant insight into the account owner’s state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a



plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

82. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

83. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

84. This Application seeks a Warrant to search all responsive records and information under the control of Apple, a provider subject to the jurisdiction of this court, regardless of where Apple has chosen to store such information. The government intends to require the disclosure pursuant to the requested Warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Apple's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

### **CONCLUSION**

85. Based on my training and experience, and the facts as set forth in this Affidavit, I submit that there is probable cause to believe that on the computer systems in the control of

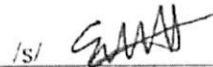
Apple there exists evidence, instrumentalities, and/or fruits of a crime. Accordingly, I respectfully request that the Court issue the proposed Warrant.

Respectfully submitted,



Special Agent Robert Glore  
United States Secret Service

Attested to by the applicant in accordance with the requirements of  
Fed. R. Crim. P. 4.1, by telephone  
on this date May 3, 2021



Elizabeth W. Hanes  
United States Magistrate Judge

**ATTACHMENT A**  
***Property to Be Searched***

This Warrant applies to information associated with the following accounts (hereafter “the TARGET ACCOUNTS”), **from June 1, 2018, to the present**, that are stored at premises controlled by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA:

Account Name	Case Number
<u>creeptor@icloud.com</u> (Target Account 1)	3:21-sw- <u>57-1</u>
<u>creeptor.ipad@icloud.com</u> (Target Account 2)	3:21-sw- <u>57-2</u>
<u>v_muradyan@icloud.com</u> (Target Account 3)	3:21-sw- <u>57-3</u>
<u>nataliyaohana777@icloud.com</u> (Target Account 4)	3:21-sw- <u>57-4</u>
<u>prizegarnitskyj5@gmail.com</u> (Target Account 5)	3:21-sw- <u>57-5</u>
<u>eliz-78@mail.ru</u> (Target Account 6)	3:21-sw- <u>57-6</u>
<u>creeptor.tab2@gmail.com</u> (Target Account 7)	3:21-sw- <u>57-7</u>



**ATTACHMENT B**  
***Particular Things to be Seized***

**I. Information to be disclosed by Apple (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period from June 1, 2018, to the present:**

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account number);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (UDID), Advertising Identifiers (IDFA), Global Unique Identifiers (GUID), Media Access Control (MAC) addresses, Integrated Circuit Card ID numbers (ICCID), Electronic Serial Numbers (ESN), Mobile Electronic Identity Numbers (MEIN), Mobile Equipment Identifiers (MEID), Mobile Identification Numbers (MIN), Subscriber Identity Modules (SIM), Mobile Subscriber Integrated Services Digital Network Numbers (MSISDN), International Mobile Subscriber Identities (IMSI), and International Mobile Station Equipment Identities (IMEI);
- c. The contents of all emails associated with the account including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

- d. The contents of all instant messages associated with the account including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;
- e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;
- f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;
- g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;
- h. All records pertaining to the types of service used;
- i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and
- j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).
- k. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
- l. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored; and

- m. Identify all linked accounts based on common telephone number, any accounts identified in Attachment A used as a secondary, alternate or recovery account, or a common machine cookie that may have been linked to one of the accounts listed in Attachment A within 30 days prior to the issuance of this warrant

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all seized information authorized by the Warrant for as long as is necessary for authentication purposes.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, instrumentalities or evidence of violations of federal criminal law, including access device fraud (18 U.S.C. § 1029), unauthorized computer access (18 U.S.C. § 1030), conspiracy, (18 U.S.C. § 371), and conspiracy to commit wire and bank fraud (18 U.S.C. § 1349)), for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Records and information relating to the laundering of criminal proceeds, the creation and maintenance of financial accounts, financial transfers and transactions, the possession of monetary instruments, and the disbursement of funds;
- b. Records and information relating to the unauthorized access of computers or computer networks;
- c. Records and information relating to stolen credit and/or debit card numbers and personally identifiable information;
- d. Records and information relating to the use of online monikers, and the use of cybercrime forums.
- e. Records and information relating to access of (*e.g.*, username, password, or location) and transactions on cybercrime infrastructure such as cybercrime forums, servers used to commit cybercrime, cybercrime services, botnet access panels, electronic payment and banking accounts, electronic mail accounts and others;
- f. Records and information relating to the identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);



- g. Records and information indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- h. Records and information that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and
- i. Records and information relating to the subscriber's state of mind as it relates to the crimes under investigation.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS  
PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Apple INC (Apple), and my title is \_\_\_\_\_. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Apple. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

1. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Apple, and they were made by Apple as a regular practice; and
2. such records were generated by Apple's electronic process or system that produces an accurate result, to wit:
  - a. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true duplicates of the original records; and
  - b. the process or system is regularly verified by Apple, and at all times pertinent to the records certified here the process and system functioned properly and normally.

3. I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature